International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Leveraging Fog Computing for a Secure and Smart Healthcare

A. Divya Preetha, T.S. Pradeep Kumar*

Abstract*: *From hairbrushes to scales, all devices have sensors embedded in them to collect and communicate data. Smart Healthcare is proving to be an exciting and dynamic area with lots of room for new innovations and the increasing consumer demand for proactive health monitoring devices. Having India poised to spend a lot on healthcare, recent innovations using IoT devices and big data analytics can propel the healthcare industry into the future. Smart healthcare providers are leveraging cloud computing with fog computing to optimize their healthcare services. These smart healthcare applications depend mainly on the raw sensor data collected, aggregated, and analyzed by the smart sensors. Smart sensors these days generate myriad amount of data like text, image, audio, and video that require real-time or batch processing. Aggregating these diverse data from various types of resources remains a dispute till date. To resolve this issue, we have proposed a softwarized infrastructure that integrates cloud computing and fog computing, message brokers, and Tor for supple, safe, viable, and a concealed IoT exploitation for smart healthcare applications and services. Our proposed platform employs machine-to-machine (M2M) messaging, data fusion and decision fusion, and uses rule-based beacons for seamless data management. Our proposed flexBeacon system provides an IoT infrastructure that is nimble, secure, flexible, private, and reasonable. We have also proposed an M2M transceiver and microcontroller for flawless data incorporation of smart healthcare applications and services. Based on the IoT devices' technical capabilities and resource availability, some systems are capable of making use of homomorphic encryption and zero knowledge proofs. The proposed flexBeacon platform offers seamless management and data aggregation without loss of accuracy. The cost of implementing a softwarized IoT for smart healthcare is also greatly reduced.

Keywords: Internet of Things, Blockchain, Tor, flexBeacon, Softwarization, Aggregation.

I. INTRODUCTION

Cryptography was born in a far away land named Egypt by its priests, nearly 4000 years ago. Modern cryptography was born in the late 1970s [1]. Key agreement protocol was named by Diffie and Hellman in 1976. RSA was introduced by Rivest, Shamir and Aldeman in 1977. Data Encryption Standard (DES) was also issued in 1977 by NIST. Public Key Infrastructure (PKI) was used in the late 1990s. The origin of Internet of Things goes back to the end of the previous millennium, just beyond RFID [2]. Some technologies like sensors, ATMs, RFIDs, and a few other innovations introduced the concept of connecting devices and things. The phrase "Internet of Things" was first named in 1999 by Kevin Ashton. Gartner's definition articulates that "The IoT is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment".

The seven main characteristics that define IoT include ecosystem, connectivity, things, data, communication, intelligence, and action. Data is the most crucial characteristic in Internet of Things. Any data is useless until it is turned into meaning and intelligence [20]. The data collected by the sensors should be communicated so that it can be tuned into actionable information, knowledge or wisdom. Despite the scope of any project, there lies a degree of automation always. There is a mounting attention for the Internet of Things these days and there are numerous reasons behind it.

Internet of Things have many flavors – Industrial Internet of Things, Internet of Everything, and Consumer Internet of Things. The Industrial Internet Consortium has delineated Industrial Internet of Things as "machines, computers and people enabling intelligent industrial operations using advanced data analytics for transformational business outcomes". Some key elements of Industrial IoT include intellectual machines, sophisticated analytics and natives at employment. The crucial part in the Industrial IoT has always been the amalgamation of IT (Information Technology) in addition to OT (Operational Technology). Consumer Internet of Things focuses mainly on innovative and engrossing customer-centric experiences. Some of the most widely used applications include fitness and personal health, smart meters, etc. The crucial thing in CIoT is that nearly 47% of the consumers worry about the privacy and security issues on the subject of IoT. The idiom "Internet of Everything" was first named by CISCO. Internet of Everything fetches people, processes, data, and things as one to craft set of connections further pertinent and expensive than ever before-twisting information into accomplishments so as to generate new competence, richer occurrences, along with unprecedented monetary opening for commerce, individuals, and countries. The key elements in Internet of Everything include citizens, processes, information and things.

Revised Manuscript Received on 30 July 2019.
* Correspondence Author
A. Divya Preetha*, School of Computing Science and Engineering, VIT University, Chennai, India.
T.S. Pradeep Kumar*, School of Computing Science and Engineering, VIT University, Chennai, India.

Internet of Robotic Things can be a model in which intellectual gadgets are capable of observing events, blend sensor data from an assortment of basis, exploit confined and distributed intelligence to settle on an unsurpassed strategy, and then proceed to be in charge of or maneuver objects of the physical world, and in some cases, while actually passing through that world. Few of the top industries that drive the Internet of Things include manufacturing, retail, government and cities, buildings and facilities, healthcare, utilities and energy, automotive, transportation, agriculture, logistics and more.

A. Smart Healthcare

New technologies are influencing our daily life in several aspects [19]. Healthcare system in these days makes use of Information and Communication Technology (ICT) to develop the eminence of health services. Blue Stream Consultancy [3] defines smart healthcare as "the technology that leads to better diagnostic tools, better treatment for patients, and devices that improve the quality of life for anyone and everyone." Some essential building blocks of smart health clinch eHealth along with mHealth services, smart home services, and electronic documentation management, in addition to intellectual allied medical devices. World Health Organization defines the name eHealth as the "use of Information and Communication Technology in support of healthcare. Examples comprise treating patients, organizing research, enlightening the health personnel, monitoring diseases and screening public health". Mobile Health or mHealth is a constituent of eHealth. The Global Observatory of eHealth (GOe) portrays mHealth as a "medical and public health practice supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices". Some broad application areas [4] in smart healthcare include Image Management, Visualization, Health Care Delivery System, Population Health Management, HealthCare Asset Tracking, and Patient Flow Analysis. Some of the key challenges [5] in implementing a Smart HealthCare include diminishing outfitted overheads, eliminating system inaccuracy, illness supervision, boosting patient familiarity, enhanced administration of medicines, and humanizing healing upshots.

According to ReportsnReports.com, smart healthcare segment is estimated to mature by 25% annually from 2016 through 2020. A part of this intensification will be due to electronic health records as well as through the use of big data analytics to make healthcare related processes more accurate and efficient. The future of Smart Healthcare is intertwined with Internet of Things. Personalized health monitoring can be achieved with the help of IoT devices. These devices work like a fitness tracker by monitoring the number of steps taken, heart rate, sleep quality, calories burnt, distance walked and then prepares a report of our personal score that ensures that the activities you are doing are healthy for you [6]. There are several apps in the medical field that empower the patients to email the results of their ECGs to their doctors, thereby saving a lot of time and work. A few customers are more willing to share their personal health data with companies and healthcare providers.

II. PROBLEM STATEMENT

The smart services and applications used by the healthcare industry will oblige the acquisition, aggregation, and scrutiny of raw sensor data. These devices will generate large amount of data, which requires pseudo-real, batch or real time processing. Aggregating assorted data from dissimilar sources is a serious issue. To address this concern, we have proposed a nimble, Softwarized infrastructure that squeezes cloud along with fog computing, Tor, message brokers, and blockchain in favor of sheltered, viable, and lithe IoT exploitation for a smart healthcare system. We have developed an unusual proposal by means of machine-to-machine contact, rule-based beacons in support of flawless data administration. We have also employed data fusion along with decision fusion to assist those smart-healthcare purposes.

III. IMPLEMENTATION

Our proposed architecture in support of smart healthcare plus services can be seen in Figure 1. Smart sensors form the basis of our model since they monitor the patients' health status, process them and record the raw sensor data. Transceivers within these smart sensors commune with the base station by means of a wireless interface. Potential base stations are elected to operate as sink nodes, data aggregators, or gateways to the cloud [7]. Connectivity is established when the IoT gateway [8] integrates with an assortment of devices and the involved network protocols.

A. Softwarization

Sensor networks are usually designed to be application-specific and hence they can't be configured dynamically. However, with the help of software-defined networking (SDN), we can perk up a sensor network's flexibility and agility. SDN achieves this by decoupling a network's data and control planes. SDN manages the data forwarding rules, thereby improving interoperability among the communication protocols [9], reducing the network deployment cost, configuring and managing by permitting the users to straightforwardly formulate industrial off-the-shelf (COTS) hardware SDN compliant [10].

COTS hardware can also be programmed by the softwarized infrastructure to perform several network functions, and to deliver end-to-end services [11] by means of NFV (Network Functions Virtualization). Softwarized Infrastructure can be connected to the VNFs to compile a service. SDN controller can be used to steer the traffic involving the physical as well as virtual network functions in addition to applications. VNFs can be created, configured, managed and monitored by the software NFV manager and

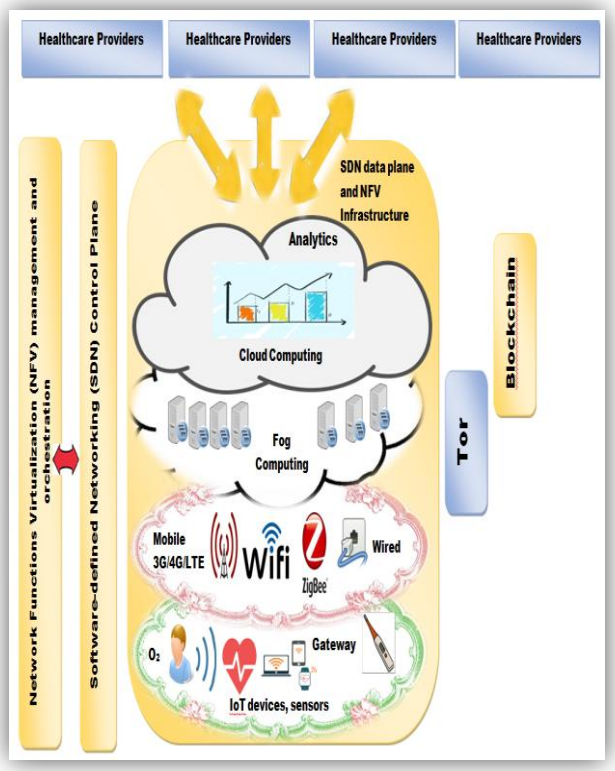

Fig 1: Architecture Diagram of a Softwarized Infrastructure for Smart Healthcare

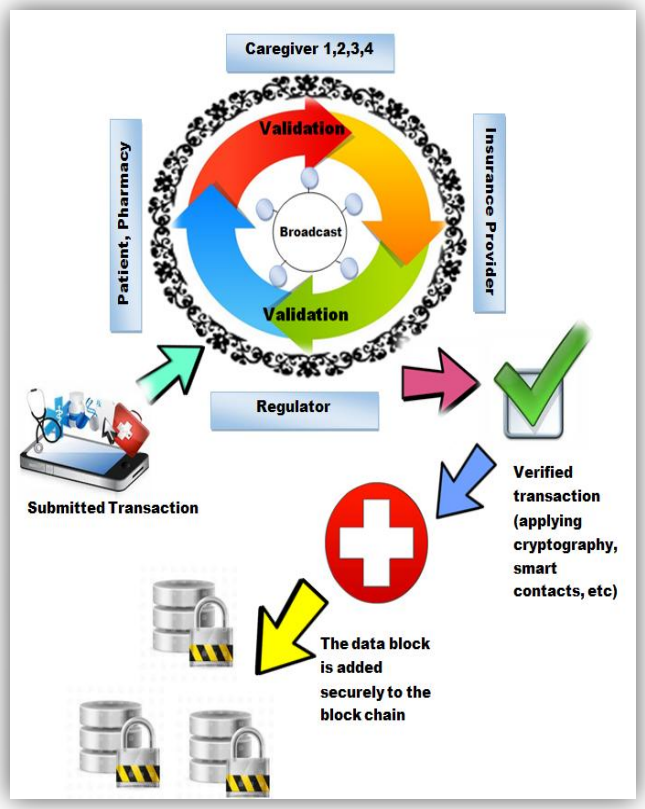

Fig 2: Securing patients' records using the Blockchain Technology

orchestrator. IoT gateways can connect to the VNFs directly or indirectly, thereby promoting nimble and commercial application and service delivery.

Our proposed system optimizes healthcare delivery [12] via analytics by enabling premature discovery and avoidance of the patients' health risks, thereby improving healthcare-delivery meticulousness. Cloud integrates patient records with genomic, biometric, social and familial data [13] and gives a clear outlook of patients' physical, mental and societal eminence. The system can in addition identify resource exploitation, thereby reducing capital and operating overheads.

B. Security and Privacy

Our proposed system protects the privacy of patient data and the erstwhile health information by using Tor [14], [15] in tandem with MQTT (Message Queue Telemetry Transport). Tor can safeguard patients and data anonymity by commanding a superimpose network of safe and sound connections between the sensor nodes and selecting random communication paths. The worst part is that Tor will introduce unpredictability and communication delays [16]. The proposed system addresses this challenge by introducing Tor between the fog nodes and the cloud.

Security of the patient records is guaranteed by the Blockchain technology which tracks and authorizes right of entry to those top secret medical records, as shown in Figure 2. Some papers [19] addressed the secure medical dispenser that is delivered via IoT device where the data is retrieved from the cloud. Blockchain is a distributed and decentralized database whose main purpose is to validate, record, timestamp, and maintain all the dealings within a reliable peer-to-peer association of systems. The scheme employs public key cryptography to restrict the transactions only to authenticated participants.

The visibility of the transaction blocks is restricted to partaker such as caregivers, pharmacies, hospitals, regulators, insurance companies, and patients. This makes it tricky for adversaries to modify the data or transactions in a passive manner. Moreover, this system lacks centralized point of vulnerability that could be exploited by hackers.

C. Latency

Most of the healthcare applications won't be in a position to afford the latency caused by the cloud. Fog computing can be employed to fill the gap in such cases. The fog nodes may be less significant in dimension and possessions than those cloud nodes but they are more powerful and efficient that IoT devices and gateways. Such a system with low latency and high performance will be capable of processing and aggregating localized data efficiently. It might also reduce any pointless passage to the cloud.

D. Data Aggregation

The acquired sensor data must be aggregated to carry out analytics, requests, along with

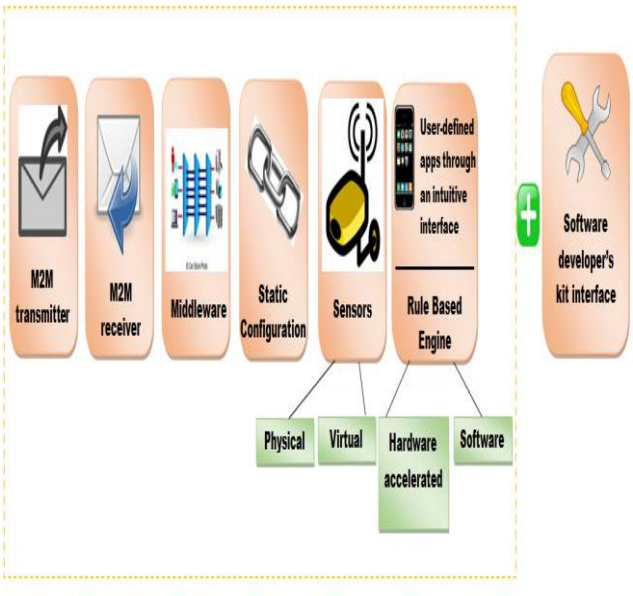

Fig 3: flexBeacon Platform

services. We have illustrated this amid a simple use case in which there are two separate sensor networks as a part of an IoT system whose main objective is to monitor cardiology patients. In order to perform healthcare analytics, this application must execute real-time scrutinizing and registration of serene information in the cloud. The application must also offer real-time alerts whenever it identifies health crisis.

The first sensor network consists of ECG (electrocardiogram) sensors for measuring the electrical signals that have power over the expansion and contraction of a heart. The second sensor network includes PPG (photoplethysmogram) sensors that sense the blood flow rate using light.

E. Data Processing

The two main data processing techniques are data fusion in addition to decision fusion. During data fusion, the sensors will pass on unprocessed information to the gateway or base station, which then sieves the information and provides a verdict concerning the patient. The verdict can be either concerning the connotation of any health constraint like the blood-oxygen level or concerning if any health circumstance necessitates concentration. The gateway subsequently throws the decision information enroute for the IoT gateway intended in favor of further cataloguing and coverage.

Within decision fusion, each sensor will in the vicinity process its individual unprocessed measurements and come up with a decision about the patient's health i.e., the status of the patient's heart. ECG sensors will pass on information to the ECG gateway. PPG sensors will collect a patient's blood-flow-rate; moreover, send them to the IoT gateway. This gateway will aggregate and process the decision regarding each patient's heart as well as will log them in cloud servers to perform analytics and state it to sanctioned personnel's mobile devices. Power efficiency though is not a concern for the gateway but there are some works that handles data from the sensors in a power efficient way that enables the data aggregation process easier. [20] designs a power efficient framework for handling data from the sensors.

Employing data fusion or else decision fusion within an IoT system has its own advantages and disadvantages. Data fusion gobbles up more power and bandwidth than decision fusion since it transmits huge volumes of data via radio. Most of the sensors may not have perfect processing capabilities and this makes decision fusion to be less precise. However, data fusion is more accurate because its computation will happen usually on more powerful gateway nodes.

F. Agile IoT Platform

A new platform named flexBeacon is proposed here which exploits a deep field-programmable gate array in the midst of hardware and software constituents. This platform utilizes M2M communications and delivers location- and context-aware services.

flexBeacon provides us with a scheme that can adapt with an assortment of hardware in such a way that any type of sensor or actuator can attach to it. This facility allows us to share access to remote control and telemetry services. The healthcare providers will also be able to construct regulations and data-flow sculpts for customizing healthcare surveillance and control functions.

flexBeacon will also facilitate mentioning specific protocols and logic to control the data flow for tracking those applications and systems that control the actuation of therapeutic gadgets like insulin pumps. M2M communication along with FPGA hardware will not only perk up the system's data gathering, aggregation in addition to exposure, but also reduce its latency.

The proposed flexBeacon platform offers seamless management and data aggregation without loss of accuracy. The cost of implementing a Softwarized IoT for smart healthcare is also greatly reduced.

IV. RESULT ANALYSIS

Our proposed flexBeacon system provides an IoT infrastructure that is nimble, secure, flexible, private, and reasonable. This platform utilizes M2M communications and delivers location- and context-aware services. flexBeacon provides us with a scheme that can adapt with an assortment of hardware in such a way that any type of sensor or actuator can attach to it. This facility allows us to share access to remote control and telemetry services. The proposed flexBeacon platform offers seamless management and data aggregation without loss of accuracy. The cost of implementing a softwarized IoT for smart healthcare is also greatly reduced. Employing data fusion or else decision fusion within an IoT system has its own advantages and disadvantages. Data fusion gobbles up more power and bandwidth than decision fusion since it transmits huge volumes of data via radio.

Most of the sensors may not have perfect processing capabilities and this makes decision fusion to be less precise. However, data fusion is more accurate because its computation will happen usually on more powerful gateway nodes. We have also proposed an M2M transceiver along with microcontroller for flawless data integration of smart healthcare applications and services. The proposed flexBeacon platform offers seamless management and data aggregation without loss of accuracy. The cost of implementing a softwarized IoT for smart healthcare is also greatly reduced.

V. CHALLENGES

A. IoT Softwarization

Softwarized IoT systems must seamlessly integrate with 5G wireless technology to achieve ultra-low latency. Lack of a standard 5G definition degrades the performance of such integration [17].

Some other concerns include managing spectrum, resources, and communication power; acquiring optimal associations sandwiched between transceivers, network devices, in addition to physical constituents like routers, sensors along with fog nodes. In order to ensure horizontal and vertical scalability, we need to gain knowledge of how to devise and manage distributed controllers and network functions.

B. Security and Privacy

The two main disputes include guarding data from malevolent traffic investigation, and recuperating obfuscation at the same time as maintaining transaction privacy as well as accountability. These issues can be resolved by employing secure communication protocols between blockchain members or IoT devices. Based on the IoT devices' technical capabilities and resource availability, some systems are capable of making use of homomorphic encryption and zero knowledge proofs [18].

For a large-scale deployment to be successful, a suitable and logical blockchain implementation anchored in smart contract is required. This can improve the system performance by minimizing the number of blocked transactions. Flex Beacon provides us with a scheme that can adapt with an assortment of hardware in such a way that any type of sensor or actuator can attach to it. This facility allows us to share access to remote control and telemetry services. Lack of proper agreement among the blockchain members that are destined to perform a requested transaction can block a transaction. We can establish participant rules and can control misbehavior by integrating some legal terms into those smart contracts.

VI. CONCLUSION

Internet of Things serves as the key player in healthcare by providing better therapeutic amenities to the patients, doctors and the hospitals. Smart healthcare applications are capable of executing concurrent patient health monitoring and using cloud based analytics, thereby improving the quality of healthcare, and the overall patient experience. Our proposed flexBeacon system provides an IoT infrastructure that is nimble, secure, flexible, private, and reasonable. We have also proposed an M2M transceiver and microcontroller for flawless data incorporation of smart healthcare applications and services. Based on the IoT devices' technical capabilities and resource availability, some systems are capable of making use of homomorphic encryption and zero knowledge proofs. Employing data fusion or else decision fusion within an IoT system has its own advantages and disadvantages. Data fusion gobbles up more power and bandwidth than decision fusion since it transmits huge volumes of data via radio. Most of the sensors may not have perfect processing capabilities and this makes decision fusion to be less precise. However, data fusion is more accurate because its computation will happen usually on more powerful gateway nodes. The proposed flexBeacon platform offers seamless management and data aggregation without loss of accuracy. The cost of implementing a Softwarized IoT for smart healthcare is also greatly reduced.

REFERENCES

1. Nisarg Desai, (2018, March 19)"Why PKI will secure the Internet of Things for years to come". Available: https://www.helpnetsecurity.com/2018/03/19/pki-iot/
2. The Internet of Things (IoT) – Essential IoT Business Guide. Available: https://www.i-scoop.eu/internet-of-things-guide/
3. ActiveAdvice. (2017, March 28). What is Smart Health and How do People Benefit? Available: https://www.activeadvice.eu/news/concept-projects/what-is-smart-health-and-how-do-people-benefit/
4. Experfy Projects. *Smart Healthcare.* Available: https://www.experfy.com/internet-of-things/smart-healthcare
5. Improving Lives with Softweb Smart Healthcare Solution: IoT-centric Solutions for Healthcare Providers and Patients. *IoT Connect.* Available: https://www.iotconnect.io/IoT-smart-healthcare-solutions.html
6. Codrin Arsene, Y Media Labs. (2017, February 9). 5 Reasons Why We're Excited About Smart Healthcare in 2017. Available: http://www.businessofapps.com/smart-healthcare-2017/
7. Datta. S, Bonnet. C, and Nikaen. N, "An IoT Gateway Centric Architecture to Provide Novel M2M Service," in *2014 IEEE World Forum on Internet of Things (WF-IoT 14)*, 2014, pp. 514-519.
8. Treadway. J, "Using an IoT Gateway to Connect the 'Things' to the Cloud", in *TechTarget IoT Agenda*, April 2016.
9. Granelli. F, "Software Defined and Virtualized Wireless Access in Future Wireless Networks: Scenarios and Standards," *IEEE Communications Magazine, 53*(6), 2015, pp. 26-34.
10. Caraguay. A, "SDN: Evolution and Opportunities in the Development IoT Applications," in *International Journal of Distributed Sensor Networks, 10*(5), 2014, pp. 1-10.
11. European Telecommunication Standards Institute (2013) *Network Functions Virtualisation (NFV)* Use Cases, ETSI GS NFV 001, v1.1.1.
12. (2011, December 5). *Whole System Demonstrator Programme Headline Findings: December 2011* UK Dept. Health.
13. (2016). *The Healthcare Analytics Adoption Model: A Framework and Roadmap* White Paper, Health Catalyst.
14. Mccoy. D, "Shining Light in Dark Places: Understanding the Tor Network," in *8th International Symp. Privacy Enhancing Technologies (PETS 08)*, 2008, pp. 63-76.
15. Sakai. K, "An Analysis of Onion-Based Anonymous Routing for Delay Tolerant Networks," in *IEEE 36th International Conf. Distributed Computing Systems (ICDCS 16)*, 2016, pp. 609-618.

16. Panchenko. A, Lanze. F, Engel. T, "Improving Performance and Anonymity in the Tor Network," in *IEEE 31st International Performance Computing and Communications Conference*, 2012, pp. 1-10.
17. Condoluci. M, Sardis. F and Mahmoodi. T, "Softwarization and Virtualization in 5G Networks for Smart Cities," in *EAI International Conference on Cyber Physical Systems, IoT, and Sensors Networks (CYCLONE 15)*, 2015, pp. 2-9.
18. (July 2015). *MultiChain Private Blockchain* White Paper. Coin Science Limited.
19. AJ Suganya G, Premalatha M, Anushka Sharma and Muktak Pandya, "IoT based Automated Medicine Dispenser for Online Health Community using Cloud", in *International Journal of Recent Technology and Engineering 7 (5S4)*, 2019, pp. 759-762.
20. Kumar, T.P. and Krishna, P.V., "Power Modelling of Sensors for IoT using Reinforcement Learning," in *International Journal of Advanced Intelligence Paradigms, 10(1-2)*, 2018, pp. 3-22.

AUTHORS PROFILE

A. Divya Preetha is currently working towards her Ph.D. degree in the School of Computing Science and Engineering, VIT University, Chennai Campus, India. She received the Bachelor's degree and Master's degree in Computer Science and Engineering from Velammal Engineering College, Anna University, Chennai, India, in 2014 and 2016, respectively. Her research interests include *Network and Systems Security, Security in Healthcare, Cloud Security, Internet of Things, Blockchain, Machine Learning*. She serves as an Associate Member in the *Institution of Engineers (India), The Asian Society of Researchers (ASR) and the International Association of Engineers*. She also serves as the Reviewer of several *SCOPUS Indexed Journals*

T.S. Pradeep Kumar received his PhD degree from the School of Computer Science and Engineering, VIT University, Vellore, India. He is currently an Associate Professor with the School of Computing Science and Engineering, VIT University, Chennai, India. His research interests include *Power modeling of sensors, energy efficiency of wireless networks, Vehicular Adhoc Networks (VANETs), E-learning strategies of higher education and Open source computing*. He is an ACM distinguished Speaker. In addition, he is serving as the Reviewer of various *International Journals of IEEE transactions on Educational technology, IJAIP, John Wiley, etc., and International Conferences*. He is the Member of *ACM, IEEE, Life Member of CSI, India*.